

Notice of Allowability

Application No.

09/655,230

Examiner

Jung W. Kim

Applicant(s)

CHANG, CHUNG NAN

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 29 October 2005.
2. ☒ The allowed claim(s) is/are 1-41.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date 03/2002, 01/2003
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Response to Appeal Brief

1. Applicant's arguments in the Appeal Brief filed on August 29, 2005 with respect to claims 1-41 have been fully considered and are persuasive. In particular, with regards to claims 1-41, Applicant persuasively argued that the prior art does not teach in entirety the claimed subject matter (Brief, pgs. 9-22 and 35-38). It is also noted that Applicant argues that the prior art does not teach the limitation of evaluating expressions of at least two different verification relationships; and comparing pairs of results obtained by evaluating the expressions of the at least two different verification relationships based on the special meaning which the application gives the terms "expression," "pairs," and "verification relationships" appearing on pg. 23, lines 13-16. (see Brief, pg. 36). Based on these arguments and considerations, the 102 and 103 rejections of claims 1-41 have been withdrawn.

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance: As per claims 1-39, the prior art of Hellman USPN 4,200,700, Schneier and Crandall USPN 5,159,632 disclose a protocol for cryptographic communication via a communication channel in which a sending cryptographic unit transmits onto the communication channel an encrypted ciphertext message obtained by supply both a plaintext message and a cryptographic key to a first cryptographic device, and in which a receiving cryptographic

Art Unit: 2132

unit receives the ciphertext message from the communication channel and by supplying the ciphertext message together with the key to a second cryptographic device decrypts the plaintext message therefrom, a method by which the sending unit and the receiving unit mutually establish a cryptographic key by first exchanging messages before the sending unit transmits the ciphertext message. In these protocols, a plurality of public quantities are made publicly available; the sending unit uses at least some of the plurality of public quantities in computing and transmitting to the receiving unit at least one sender's quantity; the receiving unit uses at least some of the plurality of public quantities in computing and transmitting to the sending unit at least one receiver's quantity; the receiving unit uses at least some of the plurality of public quantities and the plurality of sender's quantities in computing a session key. However, neither Hellman et al. '700 nor Crandall '632 disclose the receiving unit transmitting for storage in a publicly accessible repository a plurality of public quantities, nor do they disclose the sending unit transmitting a plurality of sender's quantities computed from at least some of the plurality of public quantities, nor do they disclose the receiving unit using the plurality of sender's quantities to compute and transmit at least one receiver's quantity. For these reasons, the inventions of claims 1-39 are not found to be obvious over the prior art of record.

3. As per claims 40 and 41, the prior art of Crandal USPN 5,581,616 discloses a protocol for communication in which a sending unit transmits onto the communication channel a message together with a digital signature, and, wherein before transmitting the message and the digital signature, a plurality of public quantities are stored in a

Art Unit: 2132

publicly accessible repository, a method by which a receiving unit that receives the message and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiver of retrieving the plurality of public quantities from the public accessible repository; using the digital signature and the plurality of public quantities; evaluating a pair of expressions to determine the validity of the signature. However, Crandell does not disclose the sender storing the public quantities in the publicly accessible repository; nor does Crandell disclose evaluating expressions of at least two different verification relationships, whereby the terms "expression," "pairs," and "verification relationships" are given the special meaning as appearing on the specification of page 23 in lines 13-16 (see also, Appeal Brief, pg. 36, 1st paragraph). For these reasons, the inventions of claims 40 and 41 are not found to be obvious over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."


Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

Art Unit: 2132

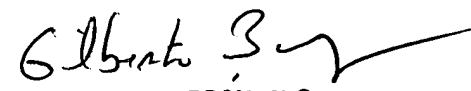
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



October 24, 2005

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100